

Remarks

In the Office Action, the Examiner noted that the claims 1-52 are pending in the application and that the claims 1-52 are rejected over various prior art references. By this response, no claims have been amended. Thus, claims 1-52 remain pending in the application. Applicant respectfully traverses the rejections for the reasons indicated below.

Applicant would like to initially inform the Examiner that Kato et al (US Patent Number 6,301,663B1) is not prior art under 35 U.S.C. 102(e) because Kato et al's earliest priority date is November 19, 1998, whereas the present application claims priority to U.S. provisional application 60/086132, filed May 20, 1998. Accordingly, for this reason above, the rejection of claims 13-15 and 38-52 should be withdrawn.

Rejections under 35 U.S.C. § 102(e) as being anticipated by Lee et al U.S. Patent No. 5,822,360

Claims 11, 28, and 29 are rejected under 35 U.S.C. §102(e) as being anticipated by Lee et al. (US Patent Number 5,822,360), hereafter "Lee".

Applicants respectfully traverse the rejection and respectfully submit that the presently claimed invention is not described by Lee et al. Applicants discuss the rejection below as it applies to (a) independent claim 11; (b) dependent claims 28 and 29.

(a) Independent claim 11

Claim 11 states in combination:

In a method for authenticating at least one of a media and data stored on said media, in order to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on said media, a data disc comprising media containing at least one modified modulation rule comprising at least one authentication key or component thereof for authenticating at least one of said media and said data, wherein said at least one of said media and said data may be outputted in at least one of an analog and audio form substantially error free and free of said at least one modified modulation rule by at least one of an error removal process and said at least one authentication key or component thereof, thereby allowing a user to experience said media without experiencing said modulation rules removed therefrom via said error removal process.

Applicant respectfully submits that the cited reference (Lee et al.) is not relevant to the above-identified claims. The cited reference does not disclose or suggest the claimed media using the methods for preventing unauthorized access of data stored on said media. Since the cited reference does not disclose or suggest the claimed methods, the invention cannot be anticipated by the cited references.

Without conceding that Lee discloses any of the features of the present invention, Lee does not disclose, for example, “a data disc comprising media containing at least one modified modulation rule comprising at least one authentication key or component thereof for authenticating at least one of said media and said data,” as recited by independent claim 11. Lee is concerned with method and apparatus for hiding auxiliary information in an audio signal for communication to a receiver and a method for recovering the auxiliary information from the output signal. (Col. 2, lines 46-48, 65-67) The system disclosed by Lee recovers the auxiliary information from the output signal by “whitening” the carrier portion of the signal followed by demodulation and decoding of FEC data to recover the auxiliary information. In contrast to the claimed invention, the apparatus using the method disclosed by Lee does not disclose the use of modified modulation rule comprising at least one authentication key.

Unlike the claimed invention, Lee discloses the use of cryptographically generated pseudorandom noise carrier to provide secure communication of the auxiliary information to a receiver. A key is needed to generate the pseudorandom noise carrier followed by demodulation and FEC decoding to recover the auxiliary information. (Col. 3, lines 3-7; Col.3, lines 66-67 to Col. 4, lines 1-7) In the claimed invention, in one embodiment of the invention, for example, the data is demodulated and analyzed/verified to determine whether the data contains broken or modified modulation rule values produced by, for example, the lookup table. The next step is to read each value and determine or derive the authentication key followed by decryption of the authentication key and error correction to recover the data. Determination or derivation of the authentication key will not occur if the modulation rule is not broken or modified. With the use of cryptographically generated pseudorandom noise carrier only a key is required to access the auxiliary information. Accordingly, Lee teaches away from the present invention.

As described above, Lee teaches nothing about, for example, a data disc comprising “media containing at least one modified modulation rule comprising at least one authentication key”. Accordingly, the combination of features of independent claim 11, when interpreted as a whole, is submitted to patentably distinguish over the reference of record.

(b) Dependent claims 28 and 29

In view of the arguments presented above for the independent claims 11, the Applicant respectfully submits that the corresponding dependent claims 28 and 29 are allowable for the reasons discussed above as well as additional limitations recited in each dependent claim also interpreted in combination.

Lee neither teaches nor suggests a data disc wherein “authentication occurs using at least three different sources for compiling compound authentication keys”, as cited in claim 28. The forward error correction (FEC) encoder suggested by Lee codes the auxiliary information in a manner such that the auxiliary information modulates the carrier in the form of FEC data. The encoder discussed by Lee does not provide means for authentication but merely provides means for ensuring the integrity of the data. Thus, as discussed above, Lee teaches away from the present invention.

Lee neither teaches nor suggests a data disc wherein “authentication occurs via decoding or decrypting the embedded authentication key or component thereof for subsequent authentication”, as cited in claim 29. The FEC decoder suggested by Lee performs the error correction necessary to produce a reliable estimate of the auxiliary data and does not provide means for authentication via decoding or decrypting the embedded authentication key. Thus, as discussed above, Lee teaches away from the present invention.

Rejections under 35 U.S.C. § 102(e) as being anticipated by Kato et al U.S. Patent No. 6,301,663B1

Claims 13, 41, and 42 are rejected under 35 U.S.C. §102(e) as being anticipated by Kato et al. (US Patent Number 6,301,663B1), hereafter “Kato”. However, the Kato patent application was filed November 19, 1998, which is after the effective filing date (May 20, 1998) of the instant application. Therefore, the Kato patent application is not prior art to the instant

application. Accordingly, for these reasons, Applicant respectfully requests withdrawal of this rejection.

In addition, Applicants also respectfully traverse the rejection and respectfully submit that the presently claimed invention is not described by Kato et al. Applicants discuss the rejection below as it applies to (a) independent claim 13; (b) dependent claims 41 and 42.

(a) Independent claim 13

Claim 13 states in combination:

In a method for authenticating at least one of a media and data to be stored on said media, in order to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on said media, a data message comprising modulation via at least one modified modulation rule to generate at least one authentication key or component thereof for authenticating said data message, and wherein the modified modulation rule cannot be readily altered, obscured nor removed from said data message without simultaneously degrading or impairing a quality of an audible component of said data message, and wherein the data message is transmitted substantially free of the modified modulation rule thereby preventing a destination processor from reading and subsequently authenticating said data message.

Applicant respectfully submits that the cited reference (Kato et al.) is not relevant to the above-identified claims. The cited reference does not disclose or suggest the claimed media using the methods for preventing unauthorized access of data stored on said media. Since the cited reference does not disclose or suggest the claimed methods, the invention cannot be anticipated by the cited references.

Without conceding that Kato discloses any of the features of the present invention, Kato does not disclose, for example, “a data message comprising modulation via at least one modified modulation rule to generate at least one authentication key or component thereof for authenticating said data message,” as recited by independent claim 13. Kato is concerned with a copy protection apparatus for preventing digital data recorded on a recording medium from an unauthorized copy from the recording medium. The copy protection apparatus disclosed by Kato comprises an encryption system and a decryption system. In contrast to the claimed invention,

the apparatus using the method disclosed by Kato does not disclose the use of modified modulation rule to generate at least one authentication key.

Unlike the claimed invention, Kato discloses a disk key generated by encryption using the disk key itself, disk keys generated by encryption using n master keys, and audio data generated by embedding information necessary for generating encryption keys for subsequent audio data using electronic watermark technique. (Col. 11, lines 5-14) In the claimed invention, the data message comprises “modulation via at least one modified modulation rule to generate at least one authentication key or component thereof for authenticating said data message”, as cited in claim 13. Claim 13 also recites “wherein the modified modulation rule cannot be readily altered, obscured nor removed from said data message without simultaneously degrading or impairing a quality of an audible component of said data message, and wherein the data message is transmitted substantially free of the modified modulation rule thereby preventing a destination processor from reading and subsequently authenticating said data message.” Kato does not disclose the use of modified modulation rule to generate at least one authentication key. Accordingly, Kato teaches away from the present invention.

As described above, Kato is not prior art under 35 U.S.C. 102(e). In addition, Kato teaches nothing about data message comprising “modulation via at least one modified modulation rule to generate at least one authentication key or component thereof for authenticating said data message”. Accordingly, the combination of features of independent claim 13, when interpreted as a whole, is submitted to patentably distinguish over the reference of record.

(b) Dependent claims 41 and 42

In view of the arguments presented above for the independent claims 13, the Applicant respectfully submits that the corresponding dependent claims 41 and 42 are allowable for the reasons discussed above as well as additional limitations recited in each dependent claim also interpreted in combination.

Kato neither teaches nor suggests about data message wherein “authentication occurs using at least three different sources for compiling compound authentication keys”, as recited in

claim 41. Kato suggests the use of shared encryption key, the encryption key for encrypting the audio data sequence, the bunch of n encryption keys for encrypting the disk key, and the bunch of part master keys. (Col. 11, lines 8-14) Kato does not provide means for authentication using at least three different sources for compiling compound authentication keys, as recited in claim 41, in combination with modified modulation rule to generate at least one authentication key, as recited in claim 13. Thus, as discussed above, Kato teaches away from the present invention.

Kato neither teaches nor suggests a data message wherein “authentication occurs via decoding or decrypting the embedded authentication key or component thereof for subsequent authentication”, as recited in claim 42. The disk key suggested by Kato is used in the decryption system to decrypt the audio data generated by encryption using the disk key and the information sent to the decryption system by electronic watermark and does not provide means for authentication via decoding or decrypting the embedded authentication key. Thus, as discussed above, Kato teaches away from the present invention.

Rejection under 35 U.S.C. § 103(a) over Lee et al (U.S. Patent No. 5,822,360) in view of Sanford, II et al (US Patent Number 5,727,092)

Claims 1, 2, 8, 9, 12, 16, 17, 22, 23, 30, 35, and 36 are rejected under 35 U.S.C. §103(a) as being unpatentable over Lee et al. (US Patent Number 5,822,360) in view of Sanford, II et al (US Patent Number 5,727,092), hereafter “Sanford”. Applicants respectfully traverse the rejection and respectfully submit that neither Lee et al nor Sanford are related to the present invention, and that there is no motivation to combine the cited references to arrive at the presently claimed invention.

(a) Claims 1, 2, 12, 16, 17 and 30

Without conceding that Sanford discloses any of the features of the present invention, Sanford states, “a method of embedding auxiliary data into host data compressed by lossy compression methods that use series expansion and quantization techniques”. (Col. 2, lines 49-51) In contrast, Lee states, “A pseudorandom noise carrier is modulated by the auxiliary information to provide a spread spectrum signal carrying the information”. (Col. 2, lines 48-51) Sanford specifically discloses a method of embedding auxiliary data into host data compressed by lossy compression methods and does not disclose the use of pseudorandom noise carrier as

disclosed by Lee. Hence, there is no motivation for combining the method of embedding auxiliary data disclosed by Sanford with the carrier disclosed by Lee. In addition, even if these prior art references are combined, the combination does not result in the presently claimed invention. For example, in contrast to the claimed invention, the apparatus using the methods disclosed by Lee and Sanford does not disclose the use of a modified modulation rule comprising at least one authentication key. Thus, the prior art does not show or suggest the combination of limitations recited in claim 1.

Similar arguments apply for claims 2, 12, and 16.

Dependent claim 17 recites the system “wherein said means for deriving includes means for deriving the embedded authentication key or component thereof as a combination of on-off binary codes representing ones and zeros to represent a predetermined symbol sequence.” Sanford discloses a “method of extracting embedded auxiliary data from a digital compression representation containing integer indices representing coefficients in a series expansion approximating original data”. (Col. 3, lines 2-5) Sanford does not disclose a means for deriving the embedded authentication key from a detected modified modulation rule and hence fails to remedy the deficiencies of Lee in relation to “deriving the embedded authentication key” as claimed.

Similar arguments apply to claim 30.

(b) Claims 8, 22 and 35

Claim 8 discloses a method “wherein said authenticating step (e) further includes a step of using at least three different sources for compiling compound authentication keys.” Claim 8 depends from claim 1, and is allowable for the reasons given in connection with claims 1, 12, and 16 as well as additional limitations recited therein. Lee discloses, “Without having the same key at both the transmitter and receiver, it will not be possible to produce the same pseudorandom noise carrier.” (Col. 4, lines 2-5) Lee does not teach or suggest the use of different sources for compiling compound authentication keys. As discussed above, there is no motivation to combine the teachings of Lee and Sanford, for example, to provide a step of using different sources for compiling compound authentication keys.

Similar arguments apply for claims 22 and 35.

(c) Claims 9, 23, and 36

Claim 9 discloses a method “wherein said deriving step (c) further comprises the step of at least one of decoding and decrypting the embedded authentication key or component thereof for subsequent authentication.” Claim 9 depends from claim 1, and is allowable for the reasons given in connection with claims 1, 12, and 16 as well as additional limitations recited therein. The FEC decoder suggested by Lee performs the error correction necessary to produce a reliable estimate of the auxiliary data and does not provide means for authentication via decoding or decrypting the embedded authentication key. As discussed above, there is no motivation to combine the teachings of Lee and Sanford, for example, to provide a step of decoding and decrypting the embedded authentication key.

Similar arguments apply for claims 23 and 36.

In view of the above, Applicants respectfully submit that claims 1, 2, 8, 9, 12, 16, 17, 22, 23, 30, 35, and 36 are unobvious over the cited references and respectfully request that the rejection under 35 U.S.C. § 103(a) of these claims be withdrawn.

Rejection under 35 U.S.C. § 103(a) over Lee et al (U.S. Patent No. 5,822,360) and Sandford, II et al (US Patent Number 5,727,092) in view of Kanota et al (US Patent Number 5,418,853)

Claims 3, 18, and 31 are rejected under 35 U.S.C. §103(a) as being unpatentable over Lee et al. (US Patent Number 5,822,360) and Sandford, II et al (US Patent Number 5,727,092) as applied to claims 1, 12 and 16 above, and further in view of Kanota et al (US Patent Number 5,418,853), hereafter “Kanota”. Applicants respectfully traverse the rejection and respectfully submit that Lee et al., Sandford, II et al, and Kanota et al are not related to the present invention, and that there is no motivation to combine the cited references to arrive at the presently claimed invention.

Claim 3 discloses a method “wherein said outputting step (f) further includes the step of converting said data into a stereo analog signal without transferring, in the data, the modulation of the at least one modulation rule used to derive the embedded authentication key or component thereof.” Claim 3 depends from claim 1, and is allowable for the reasons given in connection

with claims 1, 12, and 16 as well as additional limitations recited therein. Lee relates to a pseudorandom noise carrier that is modulated by the auxiliary information to provide a spread spectrum signal carrying the information. Sanford relates to a method of extracting embedded auxiliary data from a digital compression representation containing integer indices representing coefficients in a series expansion approximating original data. Kanato was cited for its teaching of converting data into a stereo analog signal for the purpose of copy protection. However, Kanato makes no mention of outputting data that is substantially free of a modified modulation rule or modulation after authenticating using the authentication key. Thus, it is clear that Kanato and the other cited references of record provide no disclosure or suggestion that would have motivated a person of ordinary skill in the art to modify Lee or Sanford, or to make any combination of the references of record in such a manner as to result in or otherwise render obvious the combination of features, as now recited by the limitations in the independent claims, when each claim is interpreted as a whole.

Similar arguments apply for claims 18 and 31.

In view of the above, Applicants respectfully submit that claims 3, 18, and 31 are unobvious over the cited references and respectfully request that the rejection under 35 U.S.C. § 103(a) of these claims be withdrawn.

Rejection under 35 U.S.C. § 103(a) over Lee et al (U.S. Patent No. 5,822,360) and Sandford, II et al (US Patent Number 5,727,092) in view of Chou et al (US Patent Number 5,337,357)

Claims 4, 5, 19, 20, 32 and 33 are rejected under 35 U.S.C. §103(a) as being unpatentable over Lee et al. (US Patent Number 5,822,360) and Sandford, II et al (US Patent Number 5,727,092) as applied to claims 1, 12 and 16 above, and further in view of Chou et al (US Patent Number 5,337,357), hereafter "Chou". Applicants respectfully traverse the rejection and respectfully submit that Lee et al., Sandford, II et al, and Chou et al are not related to the present invention, and that there is no motivation to combine the cited references to arrive at the presently claimed invention.

Claim 4 discloses a method of claim 1 further including a step of "locating at least one modified modulation rule on at least one of a per track basis and interval basis throughout said media such that said authentication step (e) is performed for at least one of each track to be

played, throughout playback and throughout recording” and claim 5 discloses a method of claim 1 “wherein said authenticating step (e) further includes a step of authenticating using a different authentication key or component thereof for each disc track.” Claim 4 and 5 depends from claim 1, and is allowable for the reasons given in connection with claims 1, 12, and 16 as well as additional limitations recited therein. The Office Action admits that nothing in Lee or Sanford teaches or suggests using different authentication keys for each disc track and further admits that neither Lee nor Sanford teaches locating modified modulation rule per track basis such that said authentication step is performed for each track. The office action further argues that Chou remedies the above deficiencies.

Without conceding that Chou discloses any of the features of the present invention, Chou states, “different programs or combinations are encrypted using different encryption keys and different encryption algorithms which accompany the programs on the mass distributed media.” (Col. 3, lines 21-24) Unlike the claimed invention, Chou does not disclose locating modified modulation rule per track basis such that said authentication step (e) is performed for each track. Thus, it is clear that Chou does not address the deficiencies of Lee or Sanford in a manner that teaches or suggests the combination of features of the present invention.

Similar arguments apply for claims 19, 20, 32 and 33.

In view of the above, Applicants respectfully submit that claims 4, 5, 19, 20, 32 and 33 are unobvious over the cited references and respectfully request that the rejection under 35 U.S.C. § 103(a) of these claims be withdrawn.

Rejection under 35 U.S.C. § 103(a) over Lee et al (U.S. Patent No. 5,822,360) and Sandford, II et al (US Patent Number 5,727,092) in view of O’Connor et al (US Patent Number 5,745,568)

Claims 6, 21 and 34 are rejected under 35 U.S.C. §103(a) as being unpatentable over Lee et al. (US Patent Number 5,822,360) and Sandford, II et al (US Patent Number 5,727,092) as applied to claims 1, 12 and 16 above, and further in view of O’Connor et al (US Patent Number 5,745,568), hereafter “O’Connor”. Applicants respectfully traverse the rejection and respectfully submit that Lee et al., Sandford, II et al, and O’Connor et al are not related to the present invention, and that there is no motivation to combine the cited references to arrive at the presently claimed invention.

Claim 6 discloses the “step of authenticating the at least one of the data and the media via at least two different authentication keys, each of which successively must be authenticated before said data is finally output via said outputting step.” Claim 6 depends from claim 1, and is allowable for the reasons given in connection with claims 1, 12, and 16 as well as additional limitations recited therein. The Office Action admits that the combination of Lee and Sanford does not teach the data and the media via at least two different authentications keys, each of which successively must be authenticated before said data is finally output via the outputting step, and argues that O’Connor remedies the above deficiencies.

Without conceding that O’Connor discloses any of the features of the present invention, O’Connor states, “encrypting the software program files using the hardware identifier as an encryption key...decrypting the software program files using the hardware identifier as a decryption key.” (Abstract) Unlike the claimed invention, O’Connor does not disclose authenticating the data and the media via at least two different authentication keys, each of which successively must be authenticated before said data is finally output. Thus, it is clear that O’Connor does not address the deficiencies of Lee or Sanford in a manner that teaches or suggests the combination of features of the present invention.

Similar arguments apply for claims 21 and 34.

In view of the above, Applicants respectfully submit that claims 6, 21 and 34 are unobvious over the cited references and respectfully request that the rejection under 35 U.S.C. § 103(a) of these claims be withdrawn.

Rejection under 35 U.S.C. § 103(a) over Lee et al (U.S. Patent No. 5,822,360) and Sandford, II et al (US Patent Number 5,727,092) in view of Renaud et al (US Patent Number 5,958,051)

Claim 7 is rejected under 35 U.S.C. §103(a) as being unpatentable over Lee et al. (US Patent Number 5,822,360) and Sandford, II et al (US Patent Number 5,727,092) as applied to claims 1 above, and further in view of Renaud et al (US Patent Number 5,958,051), hereafter “Renaud”. Applicants respectfully traverse the rejection and respectfully submit that Lee et al., Sandford, II et al, and Renaud et al are not related to the present invention, and that there is no motivation to combine the cited references to arrive at the presently claimed invention.

Claim 7 discloses a method that “authenticates the at least one of the media and the data over a plurality of interconnected computer networks comprising at least one of a local network, global network and the Internet.” Claim 7 depends from claim 1, and is allowable for the reasons given in connection with claim 1 as well as additional limitations recited therein. The Office Action admits that the combination of Lee and Sanford does not teach authenticating the at least one of the media and the data over a plurality of interconnected computer networks comprising at least one of a local network, global network and the Internet, and argues that Renaud remedies the above deficiencies.

Renaud relates to transmitting of signed signature data file over data bus, data link, the Internet, or some other computer or data communication network or link. (Col. 7, lines 55-60) However, Renaud does not teach or suggest that the data stored on said media is modulated via at least one modified modulation rule to generate at least one authentication key. Thus, it is clear that Renaud and the other cited references of record provide no disclosure or suggestion that would have motivated a person of ordinary skill in the art to modify Lee or Sanford, or to make any combination of the references of record in such a manner as to result in or otherwise render obvious the combination of features, as now recited by the limitations in the independent claims, when each claim is interpreted as a whole.

In view of the above, Applicants respectfully submit that claim 7 is unobvious over the cited references and respectfully request that the rejection under 35 U.S.C. § 103(a) of these claims be withdrawn.

Rejection under 35 U.S.C. § 103(a) over Lee et al (U.S. Patent No. 5,822,360) and Sandford, II et al (US Patent Number 5,727,092) in view of Hogan et al (US Patent Number 5,828,754)

Claims 10, 24 and 37 are rejected under 35 U.S.C. §103(a) as being unpatentable over Lee et al. (US Patent Number 5,822,360) and Sandford, II et al (US Patent Number 5,727,092) as applied to claims 1, 12 and 16 above, and further in view of Hogan et al (US Patent Number 5,828,754), hereafter “Hogan”. Applicants respectfully traverse the rejection and respectfully submit that Lee et al., Sandford, II et al, and Hogan et al are not related to the present invention, and that there is no motivation to combine the cited references to arrive at the presently claimed invention.

Claim 10 discloses a method comprising a step of “comparing the at least one modified modulation rule comprising the at least one authentication key or component thereof, to at least one lookup table of valid modified modulation rule output values comprising the at least one authentication key or component thereof.” Claim 10 depends from claim 1, and is allowable for the reasons given in connection with claim 1 as well as additional limitations recited therein. The Office Action admits that the combination of Lee and Sanford does not teach that the comparing step further comprises the step of comparing the at least one modified modulation rule comprising the at least one authentication key or component thereof, to at least one lookup table of valid modified modulation rule output values comprising the at least one authentication key or component thereof, and argues that Hogan remedies the above deficiencies.

Without conceding that Hogan discloses any of the features of the present invention, Hogan states, “lookup encoding tables for a multiple state encoder”. (Col. 5, lines 24-25) Hogan also states “The main lookup table has code entries for symbols in four columns corresponding to four possible states of a state machine.” (Col. 5, lines 27-30) Hogan does not teach or suggest a lookup table that contains modified modulation rules comprising the at least one authentication key. Hence, there is no motivation to combine the teachings of Lee, Sanford and Hogan to provide the claimed invention. Further, the proposed combination does not even show or suggest the combinations of features recited in claim 10.

Similar arguments apply for claims 24 and 37.

In view of the above, Applicants respectfully submit that claims 10, 24 and 37 are unobvious over the cited references and respectfully request that the rejection under 35 U.S.C. § 103(a) of these claims be withdrawn.

Rejection under 35 U.S.C. § 103(a) over Kato et al (U.S. Patent No. 6,301,633) in view of Hogan et al (US Patent Number 5,828,754)

Claims 14, 15, 46, 47, 51 and 52 are rejected under 35 U.S.C. §103(a) as being unpatentable over Kato et al (U.S. Patent No. 6,301,633) in view of Hogan et al (US Patent Number 5,828,754). However, the Kato patent application was filed November 19, 1998, which is after the effective filing date (May 20, 1998) of the instant application. Therefore, the Kato

patent application is not prior art to the instant application. Accordingly, for these reasons, Applicant respectfully requests withdrawal of this rejection.

In addition, Applicants also respectfully traverse the rejection and respectfully submit that there is no motivation to combine the cited references to arrive at the presently claimed invention. Applicants discuss the rejection below as it applies to (a) independent claim 14 and 15; (b) dependent claims 46, 47, 51 and 52.

(a) Independent claim 14 and 15

Claim 14 states in combination:

A system for authenticating at least one of a media and data stored on said media, in order to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on said media, wherein said data stored on said media is modulated via at least one modified modulation rule to generate at least one authentication key or component thereof for authenticating at least one of said media and said data, wherein said at least one of said media and said data may be outputted in an analog and/or audio form substantially error free and free of said at least one modified modulation rule by at least one of an error removal process and said at least one authentication key or component thereof, said system including a data player containing a data processor comprising lookup table means for authenticating said at least one of said media and said data and for intentionally breaking standard modulation rules by which bit patterns are recorded as one or more symbol sequences on a data media, said lookup table means connected to a focus servo, tracking servo, laser, lens and mirror, together comprising a portion of a disc reader housed in a data player device.

Applicant respectfully submits that the cited reference (Kato et al.) is not relevant to the above-identified claims. The cited reference does not disclose or suggest the claimed media using the methods for preventing unauthorized access of data stored on said media.

Without conceding that Kato discloses any of the features of the present invention, Kato does not disclose, for example, “data stored on said media is modulated via at least one modified modulation rule to generate at least one authentication key,” as recited by independent claim 14. Kato is concerned with a copy protection apparatus for preventing digital data recorded on a recording medium from an unauthorized copy from the recording medium. The copy protection apparatus disclosed by Kato comprises an encryption system and a decryption system. In

contrast to the claimed invention, the apparatus using the method disclosed by Kato does not disclose the use of modified modulation rule to generate at least one authentication key. Kato was cited for its teaching of outputting data in an analog and/or audio form substantially error free and free of said at least one modified modulation rule by at least one of an error removal process and said at least one authentication key. However, Kato makes no mention of outputting data that is substantially free of a modified modulation rule or modulation after authenticating using the authentication key.

The Office Action admits that Kato does not teach that the system includes a data player containing a data processor comprising a lookup table used by the data processor in intentionally modifying at least one modulation rule by which at least one bit indicative of the modifying is generated as at least one symbol used by the system to authenticate the at least one of the media and the data stored on the media, and argues that Hogan remedies the above deficiencies. However, Hogan discloses main lookup table that has code entries for symbols in four columns corresponding to four possible states of a state machine. Hogan does not teach or suggest a lookup table that contains modified modulation rules comprising the at least one authentication key. Further, Hogan does not disclose lookup table for authenticating the data and for intentionally breaking standard modulation rules by which bit patterns are recorded as one or more symbol sequences on a data media. Hence there is no motivation to combine the teachings of Kato and Hogan to provide the claimed invention. Accordingly, the combination of features of independent claim 14, when interpreted as a whole, is submitted to patentably distinguish over the reference of record.

Similar arguments apply for claim 15.

(b) Dependent claims 46, 47, 51 and 52

In view of the arguments presented above for the independent claims 14 and 15, the Applicant respectfully submits that the corresponding dependent claims 46, 47, 51 and 52 are allowable for the reasons discussed above as well as additional limitations recited in each dependent claim also interpreted in combination.

Kato neither teaches nor suggests about data message wherein “authentication occurs using at least three different sources for compiling compound authentication keys”, as recited in claim 46. Kato suggests the use of shared encryption key, the encryption key for encrypting the audio data sequence, the bunch of n encryption keys for encrypting the disk key, and the bunch of part master keys. (Col. 11, lines 8-14) Specifically, in Kato, these encryption keys are used for encrypting an encrypted disk key encrypted using a disk key itself, encrypting the encrypted disk key encrypted using the master key, and encrypting multimedia data in which electronic watermark information serving as some of the master keys is embedded. (Col. 1, lines 45-63) Kato does not provide means for authentication using at least three different sources for compiling compound authentication keys. Thus, as discussed above, Kato teaches away from the present invention.

Kato neither teaches nor suggests about data message wherein “authentication occurs via decoding or decrypting the embedded authentication key or component thereof for subsequent authentication”, as recited in claim 47. The disk key suggested by Kato is used in the decryption system to decrypt the audio data generated by encryption using the disk key and the information sent to the decryption system by electronic watermark and does not provide means for authentication via decoding or decrypting the embedded authentication key. Thus, as discussed above, Kato teaches away from the present invention.

Similar arguments apply for claims 51 and 52.

In view of the above, Applicants respectfully submit that claims 14, 15, 46, 47, 51 and 52 are unobvious over the cited references and respectfully request that the rejection under 35 U.S.C. § 103(a) of these claims be withdrawn.

Rejection under 35 U.S.C. § 103(a) over Lee et al (U.S. Patent No. 5,822,360) in view of Chou et al (US Patent Number 5,337,357)

Claims 25 and 26 are rejected under 35 U.S.C. §103(a) as being unpatentable over Lee et al. (US Patent Number 5,822,360) as applied to claims 11 above, and further in view of Chou et al (US Patent Number 5,337,357). Applicants respectfully traverse the rejection and respectfully submit that neither Lee et al. nor Chou et al are related to the present invention, and that there is no motivation to combine the cited references to arrive at the presently claimed invention.

Claim 25 discloses that “at least one modified modulation rule is located on at least one of a per track basis and interval basis throughout said media such that authenticating is performed for at least one of each track to be played throughout playback and throughout recording” and claim 26 discloses that “authentication occurs using a different authentication key or component thereof for each disc track.” Claims 25 and 26 depends from claim 11, and is allowable for the reasons given in connection with claims 11 above as well as additional limitations recited therein. The Office Action admits that nothing in Lee teaches or suggests locating at least one modified modulation rule on at least one of a per track basis and interval basis throughout the media such that the authentication step is performed for at least one of each track to be played, throughout playback and throughout recording, and argues that Chou remedies the above deficiencies.

Without conceding that Chou discloses any of the features of the present invention, Chou states, “different programs or combinations are encrypted using different encryption keys and different encryption algorithms which accompany the programs on the mass distributed media.” (Col. 3, lines 21-24) Unlike the claimed invention, Chou does not disclose locating modified modulation rule per track basis such that said authentication step (e) is performed for each track. Thus, it is clear that Chou does not address the deficiencies of Lee in a manner that teaches or suggests the combination of features of the present invention.

In view of the above, Applicants respectfully submit that claims 25 and 26 are unobvious over the cited references and respectfully request that the rejection under 35 U.S.C. § 103(a) of these claims be withdrawn.

Rejection under 35 U.S.C. § 103(a) over Lee et al (U.S. Patent No. 5,822,360) in view of O'Connor et al (US Patent Number 5,745,568)

Claims 27 is rejected under 35 U.S.C. §103(a) as being unpatentable over Lee et al. (US Patent Number 5,822,360) as applied to claim 11 above, and further in view of O'Connor et al (US Patent Number 5,745,568). Applicants respectfully traverse the rejection and respectfully submit that neither Lee et al. nor O'Connor et al are related to the present invention, and that there is no motivation to combine the cited references to arrive at the presently claimed invention.

Claim 27 discloses, "authentication occurs using at least two different authentication key, each of which must be successively authenticated before said data is output." Claim 27 depends from claim 11, and is allowable for the reasons given in connection with claims 11 above as well as additional limitations recited therein. The Office Action admits that nothing in Lee teaches or suggests that the data and the media via at least two different authentication keys, each of which successively must be authenticated before said data is finally output via the outputting step, and argues that O'Connor remedies the above deficiencies.

Without conceding that O'Connor discloses any of the features of the present invention, O'Connor states, "encrypting the software program files using the hardware identifier as an encryption key...decrypting the software program files using the hardware identifier as a decryption key." (Abstract) Unlike the claimed invention, O'Connor does not disclose authenticating the data and the media via at least two different authentication keys, each of which successively must be authenticated before said data is finally output. Thus, it is clear that O'Connor does not address the deficiencies of Lee in a manner that teaches or suggests the combination of features of the present invention.

In view of the above, Applicants respectfully submit that claim 27 is unobvious over the cited references and respectfully request that the rejection under 35 U.S.C. § 103(a) of these claims be withdrawn.

Rejection under 35 U.S.C. § 103(a) over Kato et al (U.S. Patent No. 6,301,663) in view of Chou et al (US Patent Number 5,337,357)

Claims 38 and 39 are rejected under 35 U.S.C. §103(a) as being unpatentable over Kato et al (U.S. Patent No. 6,301,663) as applied to claims 13 above, and further in view of Chou et al (US Patent Number 5,337,357). However, the Kato patent application was filed November 19, 1998, which is after the effective filing date (May 20, 1998) of the instant application. Therefore, the Kato patent application is not prior art to the instant application. Accordingly, for these reasons, Applicant respectfully requests withdrawal of this rejection.

In addition, Applicants also respectfully traverse the rejection and respectfully submit that there is no motivation to combine the cited references to arrive at the presently claimed invention.

Claim 38 discloses that “at least one modified modulation rule is located on at least one of a per track basis and interval basis throughout said media such that authenticating is performed for at least one of each track to be played throughout playback and throughout recording” and claim 39 discloses that “authentication occurs using a different authentication key or component thereof for each disc track.” Claims 38 and 39 depends from claim 13, and is allowable for the reasons given in connection with claims 13 above as well as additional limitations recited therein. The Office Action admits that nothing in Kato teaches or suggests using different authentication keys for each disc track and does not teach or suggests locating at least one modified modulation rule on at least one of a per track basis and interval basis throughout the media such that the authentication step is performed for at least one of each track to be played, throughout playback and throughout recording, and argues that Chou remedies the above deficiencies.

Without conceding that Chou discloses any of the features of the present invention, Chou states, “different programs or combinations are encrypted using different encryption keys and different encryption algorithms which accompany the programs on the mass distributed media.” (Col. 3, lines 21-24) Unlike the claimed invention, Chou does not disclose locating modified modulation rule per track basis such that said authentication step (e) is performed for each track. Thus, it is clear that Chou does not address the deficiencies of Kato in a manner that teaches or suggests the combination of features of the present invention.

In view of the above, Applicants respectfully submit that claims 38 and 39 are unobvious over the cited references and respectfully request that the rejection under 35 U.S.C. § 103(a) of these claims be withdrawn.

Rejection under 35 U.S.C. § 103(a) over Kato et al (U.S. Patent No. 6,301,663) in view of O'Connor et al (US Patent Number 5,745,568)

Claims 40 is rejected under 35 U.S.C. §103(a) as being unpatentable over Kato et al (U.S. Patent No. 6,301,663) as applied to claim 13 above, and further in view of O'Connor et al (US Patent Number 5,745,568). However, the Kato patent application was filed November 19, 1998, which is after the effective filing date (May 20, 1998) of the instant application. Therefore, the

Kato patent application is not prior art to the instant application. Accordingly, for these reasons, Applicant respectfully requests withdrawal of this rejection.

In addition, Applicants also respectfully traverse the rejection and respectfully submit that there is no motivation to combine the cited references to arrive at the presently claimed invention.

Claim 40 discloses, "authentication occurs using at least two different authentication key, each of which must be successively authenticated before said data is output." Claim 40 depends from claim 13, and is allowable for the reasons given in connection with claims 13 above as well as additional limitations recited therein. The Office Action admits that nothing in Kato teaches or suggests that the data and the media via at least two different authentication keys, each of which successively must be authenticated before said data is finally output via the outputting step, and argues that O'Connor remedies the above deficiencies.

Without conceding that O'Connor discloses any of the features of the present invention, O'Connor states, "encrypting the software program files using the hardware identifier as an encryption key...decrypting the software program files using the hardware identifier as a decryption key." (Abstract) Unlike the claimed invention, O'Connor does not disclose authenticating the data and the media via at least two different authentication keys, each of which successively must be authenticated before said data is finally output. Thus, it is clear that O'Connor does not address the deficiencies of Kato in a manner that teaches or suggests the combination of features of the present invention.

In view of the above, Applicants respectfully submit that claim 40 is unobvious over the cited references and respectfully request that the rejection under 35 U.S.C. § 103(a) of these claims be withdrawn.

Rejection under 35 U.S.C. § 103(a) over Kato et al (U.S. Patent No. 6,301,663) and Hogan et al (US Patent Number 5,828,754) in view of Chou et al (US Patent Number 5,337,357)

Claims 43, 44, 48 and 49 are rejected under 35 U.S.C. §103(a) as being unpatentable over Kato et al (U.S. Patent No. 6,301,663) and Hogan et al (US Patent Number 5,828,754) as applied to claim 15 above, and further in view of Chou et al (US Patent Number 5,337,357). However,

the Kato patent application was filed November 19, 1998, which is after the effective filing date (May 20, 1998) of the instant application. Therefore, the Kato patent application is not prior art to the instant application. Accordingly, for these reasons, Applicant respectfully requests withdrawal of this rejection.

In addition, Applicants also respectfully traverse the rejection and respectfully submit that there is no motivation to combine the cited references to arrive at the presently claimed invention.

Claim 48 discloses a method of claim 15 further including a step of “locating at least one modified modulation rule on at least one of a per track basis and interval basis throughout said media such that said authentication step (e) is performed for at least one of each track to be played, throughout playback and throughout recording” and claim 49 discloses a method of claim 15 “wherein said authenticating step (e) further includes a step of authenticating using a different authentication key or component thereof for each disc track.” Claim 48 and 49 depends from claim 15, and is allowable for the reasons given in connection with claims 14 and 15 as well as additional limitations recited therein. The Office Action admits that nothing in Kato or Hogan teaches or suggests using different authentication keys for each disc track and further admits that neither Kato nor Hogan teaches locating modified modulation rule per track basis such that said authentication step is performed for each track. The office action further argues that Chou remedies the above deficiencies.

Without conceding that Chou discloses any of the features of the present invention, Chou states, “different programs or combinations are encrypted using different encryption keys and different encryption algorithms which accompany the programs on the mass distributed media.” (Col. 3, lines 21-24) Unlike the claimed invention, Chou does not disclose locating modified modulation rule per track basis such that said authentication step (e) is performed for each track. Thus, it is clear that Chou does not address the deficiencies of Kato or Hogan in a manner that teaches or suggests the combination of features of the present invention.

Similar arguments apply for claims 43 and 44.

In view of the above, Applicants respectfully submit that claims 43, 44, 48 and 49 are unobvious over the cited references and respectfully request that the rejection under 35 U.S.C. § 103(a) of these claims be withdrawn.

Rejection under 35 U.S.C. § 103(a) over Kato et al (U.S. Patent No. 6,301,663) and Hogan et al (US Patent Number 5,828,754) in view of O'Connor et al (US Patent Number 5,745,568)

Claims 45 and 50 are rejected under 35 U.S.C. §103(a) as being unpatentable over Kato et al (U.S. Patent No. 6,301,663) and Hogan et al (US Patent Number 5,828,754) as applied to claim 15 above, and further in view of O'Connor et al (US Patent Number 5,745,568). However, the Kato patent application was filed November 19, 1998, which is after the effective filing date (May 20, 1998) of the instant application. Therefore, the Kato patent application is not prior art to the instant application. Accordingly, for these reasons, Applicant respectfully requests withdrawal of this rejection.

In addition, Applicants also respectfully traverse the rejection and respectfully submit that there is no motivation to combine the cited references to arrive at the presently claimed invention.

Claim 50 discloses the “step of authenticating the at least one of the data and the media via at least two different authentication keys, each of which successively must be authenticated before said data is finally output via said outputting step.” Claim 50 depends from claim 15, and is allowable for the reasons given in connection with claims 14 and 15 as well as additional limitations recited therein. The Office Action admits that the combination of Kato and Hogan does not teach the data and the media via at least two different authentications keys, each of which successively must be authenticated before said data is finally output via the outputting step, and argues that O'Connor remedies the above deficiencies.

Without conceding that O'Connor discloses any of the features of the present invention, O'Connor states, “encrypting the software program files using the hardware identifier as an encryption key...decrypting the software program files using the hardware identifier as a decryption key.” (Abstract) Unlike the claimed invention, O'Connor does not disclose authenticating the data and the media via at least two different authentication keys, each of which successively must be authenticated before said data is finally output. Thus, it is clear that O'

Connor does not address the deficiencies of Kato or Hogan in a manner that teaches or suggests the combination of features of the present invention.

Similar arguments apply for claim 45.

In view of the above, Applicants respectfully submit that claims 45 and 50 are unobvious over the cited references and respectfully request that the rejection under 35 U.S.C. § 103(a) of these claims be withdrawn.

Conclusion

Applicant respectfully submits that, as described above, the cited prior art does not show or suggest the combination of features recited in the claims. Applicant does not concede that the cited prior art shows any of the elements recited in the claims. However, Applicant has provided specific examples of elements in the claims that are clearly not present in the cited prior art.

Applicant strongly emphasizes that one reviewing the prosecution history should not interpret any of the examples Applicant has described herein in connection with distinguishing over the prior art as limiting to those specific features in isolation. Rather, Applicant asserts that it is the combination of elements recited in each of the claims, when each claim is interpreted as a whole, which is patentable. Applicant has emphasized certain features in the claims as clearly not present in the cited references, as discussed above. However, Applicant does not concede that other features in the claims are found in the prior art. Rather, for the sake of simplicity, Applicant is providing examples of why the claims described above are distinguishable over the cited prior art.

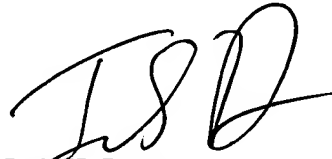
For all the reasons advanced above, Applicant respectfully submits that the rejections have been overcome and should be withdrawn.

For all the reasons advanced above, Applicant respectfully submits that the Application is in condition for allowance, and that such action is earnestly solicited.

Authorization

In the event that an extension of time is required, or which may be required in addition to that requested in a petition for an extension of time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to deposit account no. 08-0219.

Respectfully submitted

A handwritten signature in black ink, appearing to read "IHD", is written over the printed name of the signatory.

Iran H. Donner
Registration No. 35,120

Date: 3/23/04
HALE and DORR LLP
1455 Pennsylvania Avenue, NW
Washington, DC 20004
Phone: (202) 942-8400